Link: https://cutt.ly/DSaA7gN

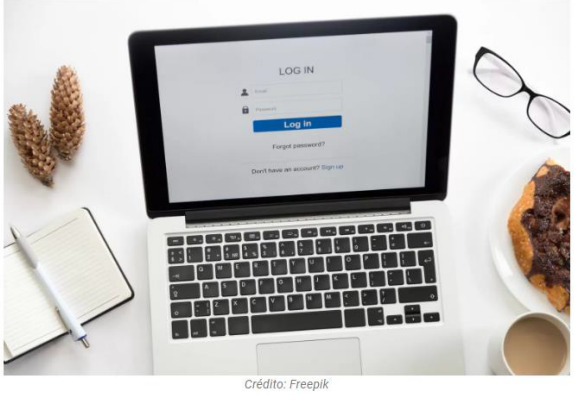
DÓLAR COMERCIAL	DÓLAR TURISMO	EURO	COTAÇÃO DE 16/03/2022 OURO NY	OURO BM&F (g)	BOVESPA	POUPANÇA	OFERECIMENTO
COMPRA: R$5,0930 VENDA: R$5,0930	COMPRA: R$5,0970 VENDA: R$5,2670	COMPRA: R$5,6358 VENDA: R$5,6385	U$1.926,36д	R$315,18 (g)	+1,98	0,6559%	

Muito além de um login e senha

COMPARTILHE

Siga no Google News

POR MARIA CRISTINA DIEZ * EM 17 DE MARÇO DE 2022 ÀS 00:27



Crédito: Freepik

Os avanços da Inteligência Artificial (AI) voltadas para a segurança da informação apontam para mudanças profundas e altamente positivas nos sistemas de *onboarding* digital. Em outras palavras, pode-se dizer que praticamente todas as inovações e tecnologias aplicadas à segurança são expostas na porta de entrada de um sistema, ainda nos procedimentos iniciais de acesso do usuário.

Isto é importante e de certa forma até lógico porque inibe as tentativas de fraude antes do acesso à plataforma. Por analogia, fazer diferente disso seria o mesmo que permitir que um intruso entre na festa para, só depois, quando ele já está lá dentro, verificar se está na lista de convidados. Essa verificação é feita ainda na entrada. Mas imagine não um, mas três portões de acesso ao "salão".

Link: https://cutt.ly/DSaA7gN

É esse o nível de segurança que o *onboarding* utiliza atualmente em muitos sistemas digitais que exigem informações delicadas do cliente. E, de fato, cada um desses 'portões' é necessário e altamente eficiente nos níveis de segurança. O primeiro deles consiste na apresentação cadastral do usuário, os dados comprobatórios necessários para que ele tenha acesso aos serviços oferecidos pela empresa, seja a conta bancária, o sistema da faculdade, a conta numa loja de *e-commerce* ou um aplicativo de investimentos, por exemplo.

Uma vez com essas informações, o sistema faz a extração e o cruzamento dos dados, com base em bancos de dados da própria empresa ou até mesmo governamentais. Isso pode ser feito por diferentes recursos de segurança digital.

No caso da prova de vida, a verificação é feita com base na leitura facial do usuário, a partir de movimentos orientados – no caso da chamada prova de vida ativa – ou com o rosto estático, se o sistema for passivo.

Essa tecnologia diferencia-se do Face Match, cuja verificação parte do comparativo entre uma *selfie* e uma fotografia respectiva de um documento de identificação. Para isso, a ferramenta faz a leitura de milhares de pontos faciais que ajudam a constatar se o portador de fato é a mesma pessoa que aparece no documento. Há não muito tempo, esse procedimento era feito humanamente, o que resultava num sinal verde para fraudadores invadirem o sistema.

Além desses há também a biometria facial, que, além das mesmas funções do Face Match, também realiza um comparativo do rosto com um banco de dados de faces, que pode ser, por exemplo, um *blacklist* da própria organização. Não por acaso, verifica-se uma quantidade cada vez maior de empresas no Brasil e no exterior que recorrem ao método para garantir a proteção do banco de dados e dos próprios clientes contra fraudes.

A partir do processo de reconhecimento, vem a terceira porta, que é a autenticação (ou não) do usuário, conferindo-lhe o acesso ao "salão". Pode ser que alguma empresa mais cuidadosa e até visionária tenha estabelecido no passado esses processos numa versão orgânica. E é de se imaginar que, se existiram, essas etapas talvez levassem algumas exaustivas horas até a conclusão. Hoje, ao falar de *onboarding* digital, estamos falando de uma inteligência que dá a resposta a tudo isso dentro poucos segundos.

Foi-se o tempo em que a segurança resumia-se a um *login* e uma senha. A tendência das plataformas *on-line* mostra que os fraudadores de hoje, embora sejam mais perspicazes do que seus antecessores, continuarão sem ter vida fácil. Nesta batalha particular entre o homem e a máquina, nós torcemos pela máquina.